(12) UK Patent Application (19) GB (11) 2 378 294 (13) A

(43) Date of A Publication 05.02.2003

(21) Application No 0119040.4

(22) Date of Filing 03.08.2001

(51) INT CL[7]
G07F 19/00

(52) UK CL (Edition V)
G4H HTG H1A H14A H14D H2T
U1S S2215

(56) Documents Cited
JP 060100868 A
US 6064990 A
US 5878337 A
US 5739512 A

(58) Field of Search
Other: Online: WPI, EPODOC, PAJ, TDB, COMPUTER

(71) Applicant(s)
Haltfern Limited
(Incorporated in the United Kingdom)
2 Mountview Court,
310 Friern Barnet Lane, Whetstone,
LONDON, N20 0YZ, United Kingdom

(72) Inventor(s)
Izidore Codron

(74) Agent and/or Address for Service
Brookes Batchellor
102-108 Clerkenwell Road, LONDON,
EC1M 5SA, United Kingdom

(54) Abstract Title
Credit card security system

(57) A credit card security system which to reduce the fraudulent use of a card. A security server 4 responds to the initiation of a card transaction 1 by instantly transmitting an SMS text message or an email, to the credit card holder's cellular mobile phone 1, or computer 8 respectively. The security server preferably includes a register of email address and mobile phone numbers which correspond to each credit card account. Alternatively, this information may be stored on the cards themselves. The card holder's mobile phone may preferably be used to respond to the message with a default stop or proceed message to stop or expedite the transaction.

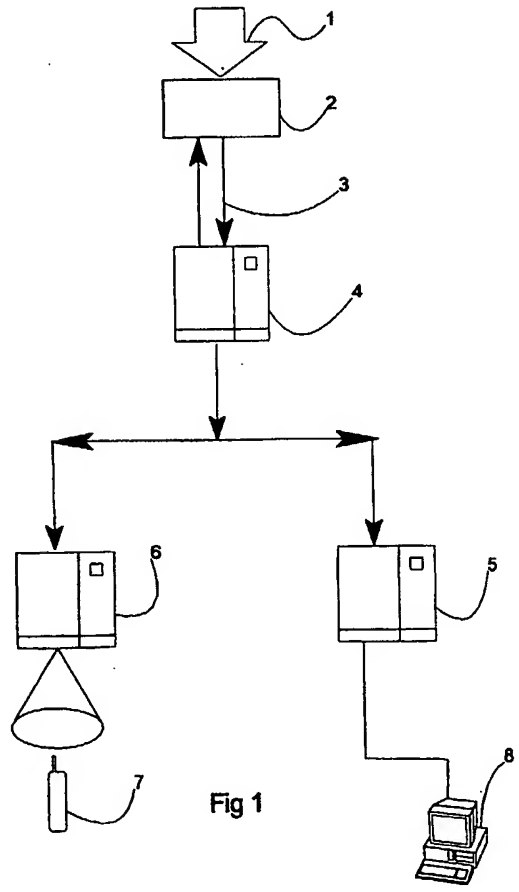

Fig 1

GB 2 378 294 A

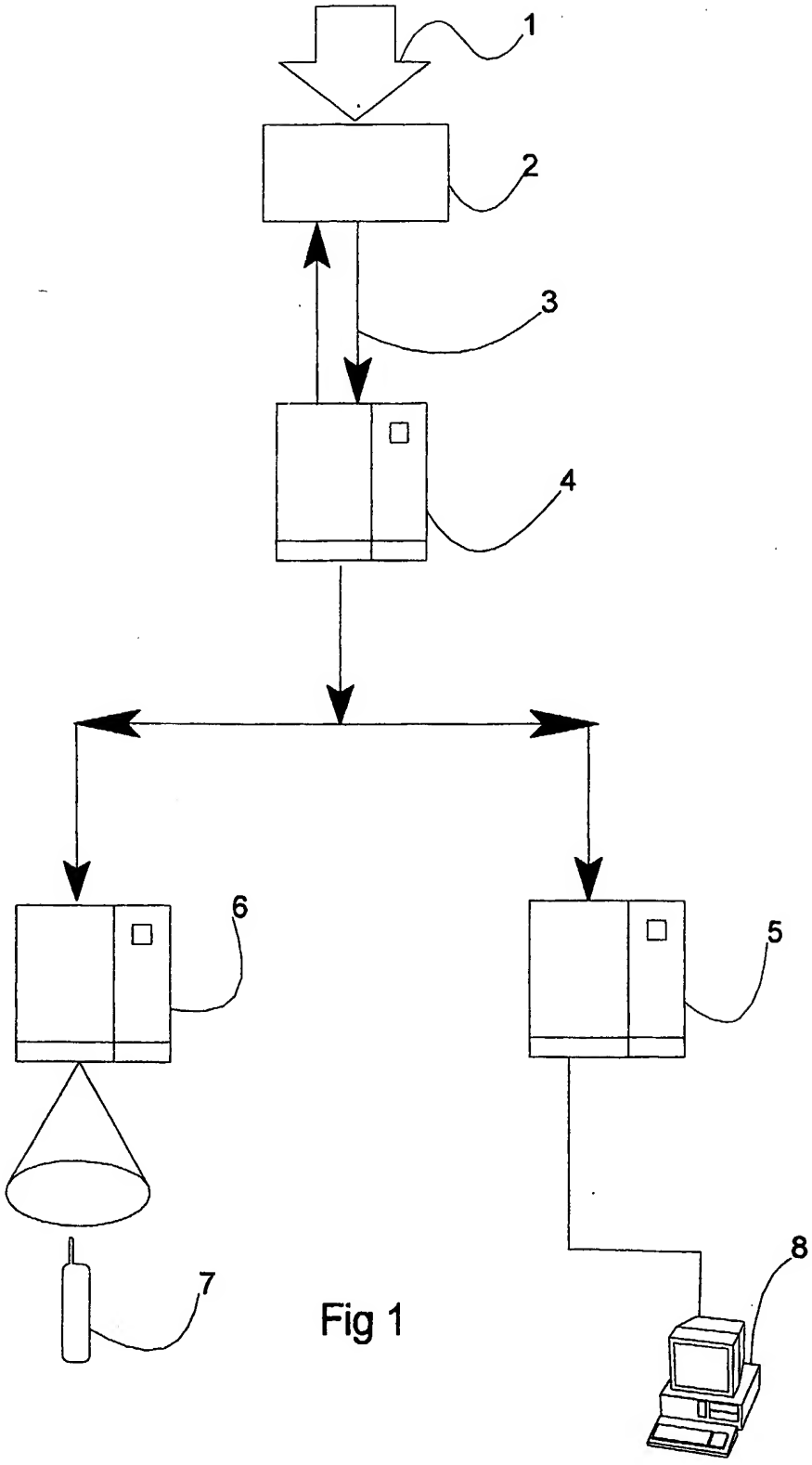

Fig 1

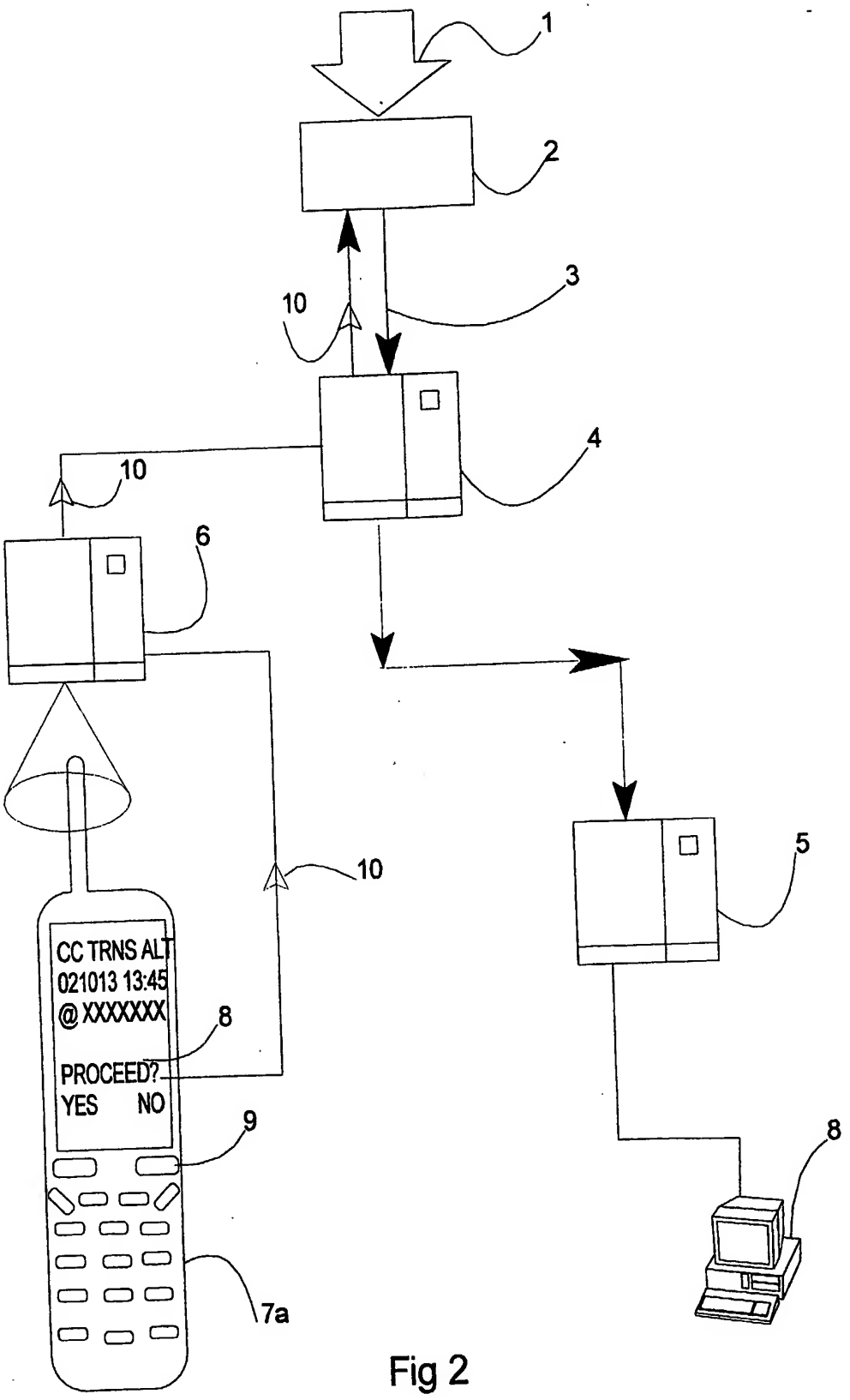

Fig 2

2378294

A Credit Card Security System.

The present invention is concerned with a credit card security system which is able to reduce the fraudulent use of a card.

The problem of fraudulent use of a credit card will be familiar to most and is becoming more serious as credit card and like transactions become more commonplace. A frequent problem results from a credit card or card data being stolen and used fraudulently for hours or even days, while the card holder is unaware of the abuse and so unable to alert the card issuer.

In the ordinary course of implementing a credit card transaction it is commonplace that the transaction will be recorded immediately to a server; if the transaction takes place in a conventional shop this is usually achieved by swiping the card through a transaction machine and the machine then addresses a remote card credit checking server provided by the credit card issuer and interrogates a database in the remote credit checking server for credit worthiness. The credit checking server will then respond by issuing signals to the transaction machine either approving the transaction or rejecting the transaction. In the case of remote transactions, it is usual that the credit card details are logged directly to a vendor's in house transaction system, either manually if the transaction is a telephone sale or directly if the sale is via the world wide web. The present invention seeks to take advantage of the existing system of processing credit card transactions and so improve credit card security at minimal cost

Accordingly the present invention provides a credit card security system having:

a credit card bearing data corresponding to a card holder account

a security server arranged to receive said card holder account data when a credit card account transaction is initiated and responsive to receipt of said data to

transmit a message immediately to at least one of a mobile phone account in the name of said card holder or an email account in the name of said cardholder.

According to a second aspect of the present invention there is provided a method of improved credit card security comprising the steps of:

initiating a transaction by communicating data corresponding to a card holder account to a vendor,

said vendor communicating said card holder account data to a security server,

said security server responding to said credit card holder account data by addressing at least one of mobile phone account data or email account data previously provided by the credit card holder, and sending at least one of an SMS message or email to said mobile phone or email account.

By immediately transmitting a message to the legitimate card holder's mobile phone and/or email account the legitimate card holder is immediately (often in a period of less than 30 seconds and usually less than 300 seconds) warned that use is being made of his card. By conventional means the credit card user may be unaware of the abuse of his card until he receives the monthly card balance probably days or weeks later, even then the abuse may not be instantly obvious. Thus the present invention gives a clear and immediate warning if the credit card account is being used fraudulently and this will give the legitimate card holder a very early opportunity to alert the credit card provider to the fraudulent use so that steps can be taken to prevent further abuse.

The mobile phone account data and/or email account data may be presented on the card in which case it is preferable that the data is encrypted and in machine readable form, such as the conventional magnetic strip or electronic memory. However, it is preferred that the credit card provider pre-loads the mobile phone and/or email account data onto the security server. The credit checking server or a server in close communication with the credit checking server may conveniently serve as the

credit checking server. In this way the mobile phone data and email account data is not available to a thief and the mobile phone and email data can be readily managed by the credit card provider in cooperation with the credit checking service provider. In this preferred embodiment of the invention the security server has means to receive said card holder account data when a credit card account transaction is initiated, memory means which holds card holder account data, and memory means holding at least one of mobile phone account data or email account data. The security server is responsive to receipt of said card holder account data to recover at least one of the mobile phone account data or email account data corresponding to said card holder account data received from memory and has transmission means to transmit a message immediately to at least one of the mobile phone account or email account corresponding to said card holder.

It is preferred that the message is a text message.

The security system and method may be further enhanced by enabling the card holder's mobile phone to respond to the message with a default stop or proceed message to stop or expedite the transaction. A stop message might then be retransmitted from the security server to the vendor so that if the transaction is fraudulent the transaction can be stopped by the vendor. Preferably the mobile phone would be adapted to present the message in a way which allows the credit card holder to respond to the message from a soft key, selecting proceed or stop, alternatively one or two of the phone keys may be used to transmit a default, proceed or stop message to the security server. The security system may be set to allow a transaction to proceed if no response is received from the mobile phone within a predetermined period, for example, ninety seconds. This will allow transactions to proceed where the mobile phone is out of service for any reason.

Embodiments of a credit card security system constructed and operated according to the system and method of the present invention will now be describe, by

way of example only, with reference to the accompanying illustrative drawings, in which:

Figure 1 is a first embodiment of the system, and

Figure 2 is a second embodiment of the invention.

Figure 1 shows a credit card transaction being implemented using the security system. At 1 data indicative of the credit card account is input to a vendor's transaction computer/server 2. The data input may be via a card reader, by manual input, direct input via internet access or by any other conventional means. This data is processed in the usual way and communicated via normal telecommunication 3 to security server provided in this example by a card credit checking server 4 in two way communication with the vendors server 2. The card credit checking server 4 includes a register of email addresses and cellular mobile phone numbers which correspond to each credit card account. Upon receipt of the credit card account data the card credit checking server addresses the corresponding mobile phone account number and/or email address and forwards a predetermined message to an internet server 5 and/or a cellular network server 6 and hence to the credit card holder's mobile phone 7 or computer 8. The message will preferably be a text message and may in addition to an indication that a transaction has been implemented include further information data such as the location, time and value of the transaction. Particularly if this further information is delivered to a PC or other handheld type device this will allow credit card holders to maintain nearly instant monitoring of their credit card account balance in addition to enhancing the security of the account.

Although this specification refers particularly to credit cards, it should be appreciated that the term credit card may also include debit cards and other forms of payment card. It may also have application where card like devices are used in smart security systems as a key to provide access to restricted areas, in such instances the unauthorised use of an authorised key would be alerted to the authorised user.

Figure 2 diagrammatically illustrates a second embodiment of the invention. The components of the system common to the first embodiment are similarly numbered and only the differences between the two embodiments will be described. When the security server 6 generates a message to the mobile phone 7a the message includes code to generate one of two response messages from the phone. Thus when a message such as that illustrated on the phone display is received it includes that the message is a "credit card transaction alert" here abbreviated to "CC TRNS ALT" the date and time and the location "@XXXXXXX" there is additionally a question "PROCEED?" 9. The message establishes a softkey 9 option "YES" to respond with a proceed message and option "NO" to respond with a stop message. In the figure, "NO" is selected which message 10 is transmitted to the cellular network server 6. The message from the phone will include code to identify the phone. This is then retransmitted to the card credit checking and security server 4 which matches the phone to the transaction in issue by correlation with a register of mobile phone account data. Thus a stop message reaches the vendor's transaction server 2 where steps may be implemented in a conventional manner to stop the transaction. The security server 4 will ordinarily wait for a period, for example ninety seconds, before emitting a proceed message based on conventional card credit criteria. Thus the proceed message may expedite a transaction. Conversely a stop message from the mobile phone or any stop transaction message based on other criteria will take priority.

Claims

1. A credit card security system having:

a credit card bearing data corresponding to a card holder account

a security server arranged to receive said card holder data when a credit transaction is requested and responsive to receipt of said data to transmit a message immediately to at least one of a mobile phone account corresponding to said card holder or an email account in the name of said cardholder.

2. A credit card security system according to claim 1 wherein the security server has;

means to receive said card holder account data when a credit card account transaction is initiated, and

memory means holding at least one of mobile phone account data or email account data addressed according to the card holder account data,

said security server being responsive to receipt of said card holder account data to recover at least one of the mobile phone account data or email account data corresponding to said card holder account data received and having

transmission means to transmit a message immediately to at least one of the mobile phone account or email account corresponding to said card holder.

3. A credit card security system according to claim 1 or claim 2 wherein the security server is provided by the credit card issuer.

4. A credit card security system according to any one of the preceding claims wherein the security server is downstream of a vendor's transaction server to receive the account data from the vendor's transaction server.

5. A credit card security system according to claim 4 wherein the security server is provided by a card credit checking server.

6. A credit card security system according to claim 1 wherein the credit card holder's mobile phone account number or email address are encoded on the credit card and the data is recoverable from the card when the card is swiped in a transaction machine by a vendor to be used by the security server in communication with the transaction machine to transmit the message.

7. A credit card security system according to any one of the preceding claims wherein the security server has means to receive a predetermined stop message from the mobile phone encoded to indicate that the transaction should be stopped.

8. A credit card security system according to claim 7 wherein the security server has means adapted to respond to receipt of a predetermined stop message to transmit a message to the vendor to stop the transaction.

9. A credit card security system according to claim 7 or 8 wherein the security server has means to receive a predetermined message from the mobile phone to indicate that the transaction should proceed, and means adapted to respond to receipt of the proceed message to send a proceed message to the vendor.

10. A method for improving credit card security when a card transaction is initiated comprising the steps of:

a card holder communicating data corresponding to a card holder account to a vendor,

said vendor communicating said data to a security server,

said security server responding to said credit card holder account data by addressing at least one of mobile phone account data or email account data corresponding to said card holder account and previously provided by the credit card holder, and sending one of an SMS message or email to said mobile phone or email account.

11. A method according to claim 10 comprising the step of the credit card issuer providing the security server.

12. A method according to either one of claims 10 or 11 wherein said security server responding to a predetermined stop message from the account holder's mobile phone by transmitting a stop message to the vendor to stop the transaction.

13. A method according to any one of claims 10 to 12 wherein the security server mobile phone is adapted to send a proceed message to the security server in response to the transaction message, said server responding by transmitting a proceed message to the vendor.

14. A method according to claim 10 wherein the mobile phone data or email data is encrypted on the credit card and comprising the step of the data being read from the credit card when the credit card is swiped in a transaction machine provided by a vendor,

said transaction machine communicating said mobile phone or email data to a server,

said server communicating an SMS message or email to the address of the credit card holder.

15. A server adapted to receive data identifying a credit card account, said server having a register preloaded with a mobile phone account number and/or email address corresponding to the holder of the credit card account, said server being adapted to respond to data indicating that a transaction is to be implemented using said credit card account by recovering a mobile phone and/or email address corresponding to the credit card account and said server being provided with communication means to issue a message to said mobile phone account or email address.

Application No: GB 0119040.4
Claims searched: 1-15

Examiner: Melanie Gee
Date of search: 25 January 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T):

Int Cl (Ed.7):

Other: Online: WPI, EPODOC, PAJ, TDB, COMPUTER

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	US 6064990	(GOLDSMITH), see Fig. 1 and col. 3 line 48 - col. 4 line 46.	1-5, 10, 11, 15
X	US 5878337	(JOAO et al.), see Fig. 1 and col. 5 line 26 - col. 7 line 49.	1-5, 7-9, 10-13, 15
X	US 5739512	(TOGNAZZINI), see Fig. 8 and col.4 lines 57-63, col. 7 lines 1-17.	1, 3, 4, 5, 6, 10, 11, 14, 15
A	JP 620100868 A	(CASIO COMPUTER CO. LTD), see abstract.	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.